REMARKS

In the first Office action

- claim 56 was rejected under 35 USC **102**, as being anticipated by Abadi et al,
- claims 52-54 were rejected under 35 USC 103 as being unpatentable over Abadi et al in view Denning et al, and
- claim 55 was rejected under 35 USC 103 as being unpatentable over Van Oorschot et al in view of Denning et al.

The only substantive change in the current office action is that

- claim 56 is rejected under 35 USC **103** as being unpatentable over Abadi et al in view of Denning et al,

Claim 56 has *not* been amended, yet the Examiner states that

> applicant's amendment necessitated the new ground(s) of rejection presented in this Office action.

Since claim 56 has not been amended, the assertion that applicant's amendment necessitated the new grounds is patently incorrect. Further, if applicant's remarks convinced the Examiner to change her mind and modify the rejection from anticipation to obviousness, applicant deserves an explanation of the reasons for the change, and an opportunity to respond. Therefore, the Office action should not have been FINAL. *Withdrawal of the finality of the rejection is respectfully solicited.*

Uncharacteristically, the current Office action begins with a "Response to Arguments" section, so the following comments pertaining to each rejection begin with a rebuttal to the Examiner's remarks.

Claim 56:

1. The Examiner states that

> section 2.3 does not disclose a 'language tutorial' as the attorney suggests. (emphasis supplied)

No such suggestion was made by applicant's attorney, but the more forceful, explicit, statement was made that "[T]he Abadi et al **article** is a language tutorial." The statement relates to the article in its entirety, and it is believed that this statement fairly characterized the article; and though the statement is not terribly material, it does explain the fact that a system having the elements of claim 56 is not described in Abadi et al.

2. In response to applicant's assertion that Abadi et al does not describe a system that includes the hardware units that are specified in claim 56, the Examiner asserts that

(a) "S represents the revocation authority" and

(b) "the first and second limitation is met by Figure 1."

Applicant thanks the Examiner for identifying the Server of Figure 1 as the "revocation authority," but since claim 56 does not claim a "revocation authority" but only a

> means for preparing a statement of an assigned revocation authority in a distributed system network in response to a policy, said revocation authority statement being associated with an initial statement.

One can only surmise that the Examiner intended to assert that the Server of Figure 1 corresponds to this means. Such an assertion necessarily means that the Figure 1 statement "2: $\{T_s, K_{ab}, \{T_s, K_{ab}, A\}_{K_{bs}}\}_{K_{as}}$" corresponds to the "revocation authority statement" of the first means of claim 56, and that the Figure 1 statement "1:A,B" corresponds to the "initial statement" of the first means of claim 56. That would be a proper correspondence, except that the Server, S, is not part of a system "in a distributed system network," as specified by claim 56.

3. As for the assertion that the second limitation is met by Figure 1, it is noted that the Figure 1 Server (a) is not in "the distributed system network", (b) it does not specify a "freshness constraint period" (emphasis supplied), (c) the message it sends is not "in response to the previously identified policy," and (e) the statement is not associated with a revocation authority statement. Figure 1 does shows one statement other than the previously accounted for statements 1 and 2; and that is statement 3:$\{T_s, K_{ab}, A\}_{K_{bs}}$. However, the only attribute that commends it to the correspondence with a "revocation authority statement" is that it is a statement. Although this statement includes a time, it does not specify a time period, it is not "in response to" a policy (no policy is even mentioned), and it is not from a revocation authority. The whole concept of a revocation authority is simply not existent in Abadi et al.

4. It is noted that the Examiner failed to rebut in the "Response to Arguments" section (and applicant believes that the Examiner was unable to rebut) the assertion that the other means of claim 56 are not taught or suggested by Abadi et al.

5. The current Office action rejects claim 56 under 35 USC 103 (as indicated above). With respect each of the "means" found in claim 56 the Examiner's rejection is a cut-and-paste copy from the first Office action.

Applicant respectfully traverses, and with the utmost respect objects to the broad brush nature of the rejection. To borrow the "needle in a haystack" idiom, it is manifestly unfair to point to a haystack, and assert that includes needle; and this unfairness is doubled when applicant previously rejected the exact same assertion, and demonstrated that the "haystack" does not have a "needle" (to the extent that is possible to prove a negative). To counter applicant's assertions, the Examiner should have identified a word, a sentence, or a paragraph that describes each of the various "means" found in the claim. The Examiner failed to do this, and applicant respectfully requests that the Examiner clearly identify – i.e., with focused citation – the means that the Examiner relies on. It is hoped that if the case is not allowed, the finality of the rejection will be withdrawn and applicant will be able to respond.

Section 2.3, which is explicitly mentioned by the Examiner, basically addresses the same protocol that Fig. 1 describes, and which is described in the right column of page 201; that is, server S receives one message from "principal A", it creates a responsive message that the server sends to A, and A sends a decrypted portion of the message received from the server to "principal B".

6. Aside from the above-mentioned fact that that Figure 1 Server in Amadi et al does not correspond to the "revocation authority" of claim 56 because it is not "in a disturbed system network," it is noted that there is no teaching that the Server prepares statement 2 "in response to a policy," which is specified in claim 56.

7. Furtherl, claim 56 specifies a

> means for preparing a validity statement ....

Clearly, the Amadi et al Figure 1 shows no "validity statement," and, hence, there is no teaching of such a means.

8. Penultimately, clam 56 specifies a

> means for selectively verifying said initial statement at said verification authority in response to said initial statement, said revocation authority statement, said freshness statement, and said validity statement.

There is nothing in Figure 1 of Amadi et al that verifies, selectively or otherwise, anything; and certainly not the initial statement.

9. Lastly, it is noted that although the rejection of claim 56 is based on Amadi et al in view of Denning et al, there is no explanation what teachings, if any, are provided by the Denning et al reference, and how that is applied to claim 56. Respectfully, an explanation is called for.

Claims 52-54:

1. Admittedly, the sentence "Time, per se, says nothing about freshness" can easily be characterized as an overstatement, but factually it is true. To illustrate, the sentence

The date this item came into being is May 2005

tells nothing about whether the item is fresh. Only if (a) another time is specified so that age can be ascertained, and (b) some other information is known that relates to what is considered fresh. For example, it is essential to one KNOW that now is November 2005, and to know what the item is before one knows whether it's fresh. If the item is milk, most people would not consider it fresh. If the item is medicine, most likely it is considered fresh.

In the case of the Abadi et al reference, all that the message provides is a time. First, one has to compare the time of the message to the time when the message is considered in order to even have chance to determine freshness. Second, one must be provided with a threshold of what is considered fresh, and what is not. The best that can be said about Abadi et al is that it implies that the time of the message is compared to the time when the message is considered, and that the threshold for determining whether the message is fresh is preset to "the start of the current authentication" (page 202, left col. lines 32-33).

In contradistinction, claim 52 specifies a step of:

> deriving freshness constraints from initial policy assumptions and an authentic statement.

This step has a number of attributes. One of them is that the freshness constraint is derived, rather than preordained. As demonstrated above, the freshness constraint in Abadi et al is preordained. Another attribute is that the freshness constraint is derived from initial policy assumptions. Certainly a freshness constraint that merely requires the

message to arrive with a time not earlier than "the start of the current authentication" is not derived from a policy consideration. Therefore, it cannot be said that Abadi et al method describes or suggests a step as the above-quoted step of claim 52.

Claim 52 also specifies a step of

> imposing freshness constraints by employing recent-secure authenticating principals to effect revocation

There is nothing in Abadi et al that teaches or suggests this step. The Examiner has not pointed to any such teaching, either in the "Response to Arguments" section, or in the section that sets forth the rejection.

As for the Denning et al equation of $|Clock - T| \leq \Delta t1+\Delta t2$, the text below the equation states that Clock is the local time, $\Delta t1$ is the difference between a clock at the source and a clock at the destination, and $\Delta t2$ plus the time delay through the network that separates the two clocks. This, however, leads to a nonsensical result because Clock, is offset from the server clock by the time it took for the message to arrive from the server, plus the difference between the clocks, so the equation can be rewritten as

$|Clock_{server} + \Delta t1+\Delta t2 - T| \leq \Delta t1+\Delta t2$, or

$|Clock_{server} - T| \leq 0$.

Clearly, that cannot be. A bit later in the text, Denning et al say that "a value of about one or two minutes for $\Delta t1$ would suffice" (page 534, col. 2, line13). *This implies that the $\Delta t1$ in this sentence is not an attribute, but a preset value, which conflicts with the definition of $\Delta t1$ provided earlier.* Modifying the expression to

$|Clock - T| \leq$ "one or two minutes"$+\Delta t1+\Delta t2$

leads to the test

$|Clock_{server} - T| \leq$ "one or two minutes."

While this **is** a reasonable freshness test, and it seems to follow the spirit of the text, it has a fixed, marker that depends on no other factor or parameter for determining freshness (the "one or two minutes") much like the marker for determining freshness that Abadi et al employ ("the start of the current authentication" test). Neither corresponds to the marker δ of claim 52, which is "a minimum necessary freshness constraint pertaining to the particular assertion" (emphasis supplied).

Based on the above, it is respectfully submitted that claim 52 is not obvious in view of Abadi et al in combination with Denning et al.

2. In connection with claim 53, the Examiner does recite "chapter and verse" in the "Response to Arguments" section, and applicant is appreciative of this. Specifically, the Examiner asserts that on page 202, 2nd paragraph, the 5th sentence says that "timestamps are used to prove that messages are fresh, and the server's message that contains encryption keys do contain a timestamp as well." That is true, and the cited sentence refers to the Server as the *trusted authority,* but the Examiner failed to correlate this fact to claim 53. It is assumed that the Examiner asserts that the server corresponds to the

> means for creating a time-stamped validity assertion message pertaining to the validity of an initial assertion

While it is true that the Server is a means for creating a time-stamped message, and the message may be labeled "validity assertion message," it is NOT true that this message pertains to the validity of "an initial assertion." The best that can be said is that this message petains to message "1: *A*,*B*", but this message says nothing about the validity of this message. Therefore, it is respectfully submitted that Abadi et al does not teach the first "means" of claim 53.

As for the second "means" of claim 53, the Examiner asserts that lines 1-21 of column 1 on page 204 teach this limitation. Applicant respectfully disagrees. The cited lines 1-21 pertain to "the message meaning rule," and "the nonce-verification rule." As indicated in applicants' previous response, the first rule says nothing about freshness, and the second rule employs freshness to determine what P – the recipient of the message – believes to be true. In the case of the Abadi et al Figure 1, that means that the second rule pertains to what happens within "principal B". But "principal B" does not assert a freshness constraint indicating a length of time, and the cited text in column 1 of page 204 also does not describe a freshness constraint that indicates a length of time. Moreover, the freshness constraint does not relate to the *initial* assertion.

As for the third means, the above comments relative to the teachings of Denning et al apply.

In light of these comments, it is believed that claim 53 is not obvious in view of the Abadi et al and Denning et al combination of references.

3. Regarding claim 54, in the "Response to Arguments" section that Examiner asserts that the limitation of the preamble is inherent in cols. 1 and 2 of page 201. More particularly, the Examiner states that

> Authentication is accomplished through the use of encryption keys and timestamps. Hence, these resources allow the authentication system to protect the authority of a distinguished principal (person, computer, or server) in a computer system.... Therefore thee three means are obvious from Abadi's disclosure.

Respectfully, this analysis is too loose. The general statement that Abadi et al use authentication through the use of encryption keys and timestamps is not focusing on the elements of claim 54 and is, therefore, not dispositive of anything relative to claim 54. Moreover, Figure 1 shows an arrangement of three systems, and if one wishes to consider them as a unit, then one might says that they constitute a "system." However, in comparing the teachings of Abadi et al to applicant's claim, which specifies a "distinguished principal," the Examiner is not free to say that the distinguished principal is a "person, computer, or server" without some asserted correspondence to some means within the reference. Stated in other words, the Examiner needs to choose and identify something that the Examiner asserts to be the "distinguished principal," the "first means," the "second means," the "third means," and the "means for verifying" that are specified in claim 54. Only then can one determine whether the Examiner's rejection is justified.

If one were to assume that the Examiner asserts that the Server of Figure 1 is the "distinguished principal" and also the "first means," applicant would not disagree. However, the method described by Abadi et al is clearly not a method "for protecting an authority of a distinguished principal and enforcing revocation when the authority is compromised" when the "distinguished principal" is the Server. If, on the other hand, one were to assume that the Examiner asserts that the "principal A" of Figure 1 (or a "person, computer, or server" that belongs to A) is the "distinguished principal," then "principal A" must be the "first means" of the claim, but "principal A" does NOT issue an "authoritative assertion" as specified in claim 54.

As suggested by the above, the Examiner has not identified any specific correspondence between any means that is taught in Abadi et al and the elements of claim 54, and applicant believed that no correspondence can be found that is on point for any of the other elements, and certainly not for all of them.

As for the Denning et al reference, applicant's view was already expressed above. Therefore, it is respectfully submitted that claims 54 is not obvious in view of the Abadi et al and Denning et al combination of references.

Claim 55:

1. As in the previous Office action, the Examiner asserts that the Van Oorschot et al reference teaches the first four "means" of claim 55, citing col. 1, lines 30-67 and col. 1, lines 1-9. The cited text is found in the "Background of the Invention" section of the reference, and consists of three paragraphs:

Paragraph 1:

> Public keys are typically distributed by means of public-key certificates (ITU Recommendation X.509:1993, hereafter ›X.509!). A public-key certificate consists of a user's distinguished name, the public key to be associated with that name, and the digital signature of a trusted third party (commonly called the certification authority or CA) which binds the name to the key. The certificate usually also contains additional fields, including a validity period, and a serial number which uniquely distinguishes all certificates from one certification authority. Effectively, the signature serves as the trusted party's guarantee that the key is associated with the specified user. When other system users successfully verify, using standard techniques (Rivest, Shamir and Adleman 1978, hereafter ›RSA!) that a certificate signature is correct, they may then be reasonably assured that the public key in the certificate is authentic, and may safely proceed to use the public key within for appropriate cryptographic applications. U.S. Pat. No. 4,405,829 (Rivest et al, Sep. 20, 1983) describes the RSA technique.

This paragraph offers a discussion of public key certificates, and what they contain. It mentions that certificates usually include information regarding the certification authority. At best, one might assert that the certificate is also a freshness constraint, and that the mentioned certification authority corresponds to the means for issuing certificates for principals, and to the means for asserting freshness constraints. None of the other means are even hinted at.

Paragraph 2:

> Public key certificates are typically stored in public databases commonly referred to as directories ›X.509!. The validity period in a certificate implies a default expiry date of the certificate, after which time all users should treat the binding between the key and user as invalid. If the certification authority which signed the certificate decides, for some reason (see below), to retract its endorsement of the

> public key prior to the normal expiry date, some method is followed to revoke the certificates. Reasons for revoking certificates may include compromise or suspected compromise of the corresponding private key, or early termination of the need for the key.

This paragraph teaches that a certificate has a validity period, following which the certificate expires, and that if the certification authority decides to retract its endorsement early, some unspecified method may be used. This paragraph does not teach about any of the means specified in claim 55.

Paragraph 3:

> One method of certificate revocation involves use of a certificate revocation list or CRL (for example, see ›X.509!). A CRL according to ›X.509! consists of a list of zero or more pairs of data items, each pair indicating a certificate serial number and the time or date at which the certificate was revoked. The composite list also includes a date of issue or validity period, and is digitally signed by the certification authority to ensure authenticity. In prior art, there is typically a single CRL associated with a certification authority, and the CRL is updated at regular intervals (e.g. daily or weekly). Before extracting for use any public key from a certificate, prudent system users verify the signature on the certificate, that the current time precedes the expiry date therein, and that the serial number of the certificate in question does not appear on the most recent valid CRL.

This paragraph describes one method of certificate revocation. There is no mention as to where this method is practiced, but the statement that the CRL is "associated with a certification authority" suggests that the method is practiced by the certification authority, which conforms to the teaching of the previous paragraph. This paragraph also does not teach any of the other means of claim 55.

In short, under the most favorable interpretation of the cited text, it still remains that there is no teaching or suggestion of a means for asserting a principal that is authorized as an authority, or a means for delegating authority. Denning et al is cited for the relation found in the "means for verifying," but applicant's view in connection with this relation has already been discussed earlier, and those views apply here. Therefore, it is respectfully submitted that claim 55 is not obvious in view of the Van Oorschot et al and Denning et al combination of references.

In light of the above remarks, it is respectfully submitted that all of the Examiner's rejections have been overcome. Reconsideration and allowance are respectfully solicited.

Respectfully,
Stuart Gerald Stubblebine

Dated: 3/28/06

By _____

Henry T. Brendzel
Reg. No. 26,844
Phone (973) 467-2025
Fax (973) 467-6589
email brendzel@comcast.net